Predictive Policing – Prädiktive Polizeiarbeit zwischen Innovationsbegeisterung und rechtlichen Schranken

Gastautor 2016-06-24T07:00:39

von ANN-KRISTIN KÄSTNER und SIMONE KUHLMANN

In einer zunehmend digitalisierten und vernetzten Welt entstehen tagtäglich Millionen neuer Datensätze, die mit Hilfe von Big Data-Anwendungen auf bislang unbekannte Zusammenhänge analysiert werden können. Dies will sich vermehrt auch die Polizei zu Nutze machen, indem sie mittels Analysesoftware Vorhersagen darüber trifft, wo eine erhöhte Wahrscheinlichkeit künftiger Straftaten oder Gefahren besteht. Ein Werbespot des US-Unternehmens IBM präsentiert eindrucksvoll, wie es derartige Software der Polizei scheinbar ermöglicht, in aller Ruhe Kaffee zu trinken und dennoch vor potenziellen Tätern am Tatort zu sein. Während sich Vorhersagesoftware in Ländern wie den USA bereits etabliert hat, steckt die Nutzung von Programmen wie „PRECOBS“ oder „PREDPOL“ in Deutschland noch in den Kinderschuhen. Von der Vorstellung einer vernetzten, ressourceneffizienten Polizei getrieben, testen, angesichts gestiegener Einbruchszahlen, derzeit einige Bundesländer Predictive Policing-Software zur Auswertung und Vorhersage von Wohnungseinbrüchen.

„I'm not going to get more money. I'm not going to get more cops. I have to be better at using what I have, and that's what predictive policing is about" – Los Angeles Police Chief Charlie Beck

Unter den Oberbegriff des Predictive Policing fallen Softwareprogramme, die Polizeidaten mit externen Datensätzen verknüpfen, um Straftaten und Gefahren mit Hilfe von Algorithmen zu prognostizieren. Ausgangspunkt sind von der Polizei erhobene anonymisierte Daten u.a. über Tatort, Tatzeit und Art der Begehung, die in Deutschland etwa mit Wetter- und Veranstaltungsdaten oder – wie in den USA – mit Zahltagen und Daten aus sozialen Medien verbunden werden. Bei der bisher in Deutschland allein auf Wohnungseinbrüche angewendeten Software werden aus diesen Daten und unter Bezugnahme auf den kriminologischen Near-Repeats-Ansatz, Wahrscheinlichkeiten für weitere ähnlich gelagerte Straftaten in einem abgegrenzten geografischen Raum in unmittelbarer zeitlicher Nähe berechnet. Das Ergebnis dieser algorithmischen Analyse ist die musterhafte Darstellung wahrscheinlicher Wohnungseinbrüche als räumlich-verortbare Delikte in einem konkret umrissenen Zeitfenster. Ziele des Einsatzes solcher Prognoseprogramme sind – sowohl strategisch als auch konkret operativ – die Antizipation sowie die Verhinderung von Straftaten und die nachhaltige Ausrichtung polizeilicher Arbeit. Im Fokus steht der effiziente Einsatz finanzieller und personeller Ressourcen.

Vernetzte Polizeiarbeit als datenschutzrechtlicher Trojaner?

Auf den ersten Blick fehlt durch die Nutzung anonymisierter Daten bei den bisher in Deutschland getesteten Prognoseprogrammen jeglicher Personenbezug und damit die Qualifizierung als Eingriff in das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Bei genauerem Hinsehen lässt der durch die Software ermittelte abgegrenzte geografische Raum bereits einen Rückschluss auf die dort lebenden oder sich aufhaltenden Personen zu. Würden – durch etwaige Ermittlungserfolge angeregt – weitere Daten v.a. aus dem Internet zur Analyse herangezogen, könnten konkrete Personen z.B. als eventuelle Täter ermittelt werden. Ein Vorbild könnte die in den USA bereits verwendete Software sein, bei der etwa Informationen über Freundschaftsbeziehungen oder verdächtige Aktivitäten aus sozialen Netzwerken gebraucht werden. Neben der mangelnden Erkennbarkeit genutzter Datenkategorien wirft die intransparente Funktionsweise der von der Software gebrauchten Algorithmen datenschutzrechtliche Fragen auf. Für Einzelne ist nicht erkennbar, wann welche sie betreffende Daten anhand welcher Kriterien verknüpft und ausgewertet werden.

Die Gefahr der heimlichen Überwachung bzw. Speicherung, v.a. nicht strafbarer Handlungen, wird von einer Zweckentfremdung der Datenerhebung und -verarbeitung begleitet, die eine Einwilligung in ebendiese unmöglich macht. Erfordert die Nutzung von polizeilich erhobenen anonymisierten Daten für Predictive Policing-Software an sich keine konkrete und enge Zweckbindung, wird sie beim Verknüpfen dieser mit ursprünglich nicht von der Polizei selbst erhobenen Daten umso bedeutsamer. Bei Einbeziehung von seitens Dritter erhobener personenbezogener Daten – bspw. aus sozialen Medien – würde der Bezug zum ursprünglichen Zweck der Datenerhebung durch Dritte fehlen.

Darüber hinaus ist angesichts der Grundsätze der Datenvermeidung und -sparsamkeit ein Blick auf die für die Prognose erforderliche möglichst lange Speicherung der verwendeten Daten zu werfen. Würden die gebrauchten Daten bzw. die Ergebnisse der Prognosesoftware eine Zuordnung zu konkreten Personen ermöglichen sowie anlasslos gespeichert werden, müssten die Vorgaben des BVerfG und des EuGH Beachtung finden. Danach bilden die Normenklarheit hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes sowie eine differenzierte anstelle einer generellen Datenspeicherung wesentliche Grundsätze. Ob an diesen Grundsätzen angesichts Big Data und der diese erst ermöglichenden gewaltigen Datenmengen festgehalten werden kann oder sich diesbezüglich zukünftig ein neues Verständnis des Datenschutzes etablieren muss, wird sich auch auf Predictive Policing-Software auswirken.

Vorverlagerung der gefahrenrechtlichen Eingriffsschwelle?

Mit Predictive Policing verschiebt sich die Polizeiarbeit einen weiteren Schritt von der Gefahrenabwehr hin zur Gefahrenverhütung. Einher geht damit die Befürchtung, dass sich die Eingriffsschwelle für polizeiliche Maßnahmen in das Vorfeld von Gefahren verlagert und Bürger anlasslos unter Generalverdacht gestellt werden.

Dies mag insofern zutreffen, als man die Prognose selbst als stigmatisierenden Effekt betrachtet und bereits die Möglichkeit polizeilicher Maßnahmen als Eingriff versteht. Die erhöhte Wahrscheinlichkeit Ziel einer polizeilichen Maßnahme wie bspw. einer Durchsuchung zu werden, allein weil man sich innerhalb eines als gefährdet identifizierten Raumes aufhält, führt unweigerlich dazu, dass das Betreten oder Bewohnen derartiger Räume ein stetes Gefühl des Verdächtig seins hinterlassen kann. Was dabei als Generalverdacht erscheint, birgt in jedem Fall die Gefahr, dass Personen aus Furcht vor negativen Auswirkungen ihr Verhalten ändern und damit letztlich in ihrer freien Grundrechtsausübung beeinträchtigt sein können.

Versteht man Predictive Policing hingegen lediglich als Erkenntnisgewinn, der die Gefahrenprognose eines erfahrenen Beamten ersetzt, wird sich die Annahme einer Vorverlagerung der Eingriffsschwelle jedoch nicht halten können. Ungeachtet des Einsatzes von Analysesystemen knüpft polizeiliches Handeln, das in Grundrechte eingreift, nach wie vor an das Vorliegen einer tatsächlichen Gefahr. Die mittels Software ermittelte Prognose ersetzt – wenn auch in qualifizierter Form – lediglich die bislang von einem Polizisten unter Zugrundelegung aller Erkenntnisquellen und anhand seiner Erfahrungssätze selbstgetroffene Einschätzung der Gefahrenlage. Predictive Policing verschiebt insofern nicht die Eingriffsschwelle, sondern ermöglicht aufgrund einer nunmehr bekannten Gefahr erst die polizeiliche Maßnahme.

Fraglich bleibt dann allerdings, inwiefern es derartigen Vorhersagesystemen überlassen werden kann, eine Prognose zu erstellen, die die Grundlage für Maßnahmen und damit für Eingriffe in die Rechte von Bürgern begründet. Ein reflektierter Umgang mit den Analyseergebnissen unter anhaltendem Einsatz von softwareunabhängigem polizeilichem Erfahrungswissen scheint erforderlich,

um einen verantwortungsbewussten Gebrauch derartiger Technologien zu gewährleisten.

Neuartige Technologie – altbekannter Interessenausgleich

Der Einsatz von Predictive Policing bietet in Zeiten zunehmender Gefahrenlagen einen möglichen Ansatz vorhandene knappe Ressourcen effizienter einzusetzen. Diese neue strategische Ausrichtung darf jedoch nicht zu Lasten des Rechts auf informationelle Selbstbestimmung in seiner jetzigen verfassungsrechtlichen Ausgestaltung gehen. Die große Herausforderung wird daher sein, ein optimales Gleichgewicht zwischen Persönlichkeitsrechten und dem Interesse an effizienterer Gefahrenabwehr und Strafverfolgung zu schaffen.
